UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/773,681	02/06/2004	Pradeep Bahl	M1103.70234US00.	7805

45840 7590 04/08/2009

WOLF GREENFIELD (Microsoft Corporation)
C/O WOLF, GREENFIELD & SACKS, P.C.
600 ATLANTIC AVENUE
BOSTON, MA 02210-2206

EXAMINER	
HUSSAIN, TAUQIR	
ART UNIT	PAPER NUMBER
2452	
MAIL DATE	DELIVERY MODE
04/08/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/773,681	BAHL ET AL.	
	Examiner	Art Unit	
	TAUQIR HUSSAIN	2452	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12-23 and 25-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10, 12-23, and 25-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 02/13/2009 has been entered.

Response to Amendment

2. This office action is in response to amendment /reconsideration filed on 02/13/2009, the amendment/reconsideration has been considered. Claims 1-10, 12-22 and 40-44 have been amended. Claims 1-10, 12-23 and 25-44 are pending for examination, the rejection cited as stated below.

Response to Arguments

3. Applicant's arguments have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. As to claims 1-2, 10, 16, 21-22 and 27 are rejected under 35 U.S.C 103(a) as being unpatentable over Tezuka (Pub. No.: US 2003/0074359 A1), hereinafter “Tezuka”

in view of Meyer (Pub. No.: US 2002/0178, 246 A1), hereinafter "Meyer" and further in view of Delo et al (Patent No.: US 6345, 386 B1).

6. As to claim 1, Tezuka discloses, acquiring at least one raw network DNA component (Tezuka, Fig.2, step-s2, [0036], where NE collects the network information), each raw network DNA component corresponding to an attribute of a computer network (Tezuka, Fig.2, step-s2, [0036], where trunk and tributary elements are computer network attributes);

generating at least one derived network DNA component according to at least one derived network DNA component specification, each derived network DNA component corresponding to an attribute of the computer network (Tezuka, Fig.2, step-S4, [0038], where based on required changes a new network model is created and [0036-0037], where new network model is build on existing network information and therefore the core attributes of the network corresponds to the same or old network), at least one of said at least one derived network DNA component specification referencing at least one of said at least one raw network DNA component (Tezuka, Fig.2, step-s4, change network management model using relevant scenario [0038], where retrieved scenario is referencing the existing model); and

determining a network DNA for the computer network (Tezuka, Fig.2, [0032], where network construction is determining a DNA for the computer network, inherently will be an ID, domain, subnet etc), the network DNA taxonomically classifying the computer network (Tezuka, [0036, lines 3-4], where trunk and tributary are taxonomically classified network architecture), and the network DNA comprising at least

one of said at least one derived network DNA component (Tezuka, [0039], where newly created network model is updated and saved into management storage space, which is a derived network DNA from existing network).

Tezuka however is silent on disclosing explicitly, testing a network DNA policy condition of a network DNA policy for satisfaction, the network DNA policy condition referencing at least one of said at least one derived network DNA component; and

An execution of a network DNA policy action of the network DNA policy if the network DNA policy condition of the network DNA policy is satisfied.

Meyer however discloses, testing a network DNA policy condition of a network DNA policy for satisfaction, the network DNA policy condition referencing at least one of said at least one derived network DNA component (Meyer, Fig.2, [0015], where analysis platform collects configuration files from the relevant network devices and builds up an internal instance of a network configuration model based on the configuration files and the network topology which relates to network DNA policy condition referencing network DNA component); and

an execution of a network DNA policy action of the network DNA policy if the network DNA policy condition of the network DNA policy is satisfied (Meyer, Fig.2, where the analysis platform receives the network policy as an input and then analyzes the network configuration model to verify that the IP traffic from and to these hosts are limited according to the type of service, and to ensure that the right type of IP traffic get from/to a host, which includes the configuration of relevant routers for switching traffic,

firewalls for passing through or dropping traffic, and local access control mechanisms on the host (e.g., TCP wrappers) for making the services accessible).

Therefore, it would have been obvious to one of ordinary skilled in the art at the time the invention was made to combine the teachings of Tezuka with the teachings of Meyer in order to provide a platform analyzer to simulate network configuration model according to the network policy and adds an entry to its final report each time that it detects a violation against the network policy in the network configuration model. The data in the entries pinpoints the cause of the deviation(s) from the network policy.

Tezuka and Meyer however are silent on disclosing explicitly that, Initiating on the computer connected to the computer network a network policy.

Delo however discloses a similar concept of, " Initiating on the computer connected to the computer network a network policy" (Delo, Abstract, where in network setting, advertised applications may be assigned to a user via a policy and obviously application is a software trigerd).

Therefore it would have been obvious to one of the ordinary skilled in the art at the time the invention was made to combine the teachings of Tezuka and Meyer with the teachings of Delo in order to provide a system for advertising software applications, such as those assigned to a user via a policy, whereby each advertised application appears available to the user even if not installed. Applications may be advertised as available from a source, even though the application is not actually installed.

7. As to claim 10, carry similar limitation as parent claim1 and therefore, is rejected under for same rationale.

8. Claims 16, 20-21 and 22, 27, 40-41 are rejected under 35 U.S.C 103 (a) as being unpatentable over Tezuka and Meyer in view of Jemes et al. (Pub. No.: Us 2001/0037384 A1), hereinafter "Jemes".

9. As to claim 16, Tezuka and Meyer discloses the invention substantially, including, performing a method comprising determining a network DNA of a computer network (Tezuka, Fig.2, Step-s2, [0036], where collecting network element information means determining Network DNA of a computer network), the network DNA comprising a network species component (Tezuka, [0036], where inherently any network will contain network species component which can merely be a network ID, domain, subnet etc) and;

providing the network DNA through an interface on the computer (Meyer, [0016], where The analysis platform receives the network policy as an input and then analyzes the network configuration model and analysis platform can be interpret as interface).

Tezuka and Meyer however are silent on disclosing explicitly "configured to indicate a network species classification, the network species classification including an enterprise network, a home network and a public network, or "provide network DNA including the network species component".

Jemes however discloses a similar concept of identifying a network architecture/topology where, configured to indicate a network species classification, the

network species classification including an enterprise network, a home network and a public network (Jemes, Abstract and [0017], where all network devices are configured to enforce the network security policy for the network to which it is connected) and "provide network DNA including the network species component" (Jemes, [0017], where network policy defines the security level of the network to which it is connected, e.g. different security level of different network as depicted in Fig.2).

Therefore it would have been obvious to one of the ordinary skilled in the art at the time the invention was made to combine the teachings of Tezuka and Meyer with the teachings of Jemes in order to provide a system which includes a plurality of networks where each network has at least one network device configured to transmit and receive data and has a network security policy. The secure network further includes a plurality of network control points where each network control point has at least one network control point device. Each of the plurality of network control points is connected to at least one of the plurality of networks.

10. As to claim 22, Tezuka and Meyer discloses the invention substantially, including, at least one computer connected to at least one computer network (Tezuka, Abstract, where inherently network model is a computer network model); and

at least one network DNA store configured to store a network DNA for at least one of said at least one computer network (Tezuka, [0038], where updated network model is stored), the network DNA taxonomically classifying said at least one of said at least one computer network (Tezuka, Fig.3, [0041], where network DNA taxonomically classified as N1, N2, N3 and N4 as access network, SDH network and IP network

respectively), and the network DNA comprising at least one derived network DNA component (Tezuka, Fig.2, Step-s4, [0038], where updated network model is a network derived DNA).

An interface configured to provide network DNA to at least one application program (Meyer, [0015], where policy modeling language "PML" or an analysis platform "Ontura server" can be equivalent to an interface between input and application program).

the at least one derived network DNA component comprising a network species component configured to indicate a network species classification (Jemes, Abstract and [0017], where all network devices are configured to enforce the network security policy for the network to which it is connected), the network species classification including an enterprise network, a home network, and a public place network (Jemes, [0017], where network policy defines the security level of the network to which it is connected, e.g. different security level of different network as depicted in Fig.2).

As to claims 21 and 27, Tezuka, Meyer and Jemes discloses the invention substantially as in parent claims 16 and 22, including, testing a network DNA policy condition of a network DNA policy for satisfaction, the network DNA policy condition referencing at least one of said at least one derived network DNA component (Meyer, Fig.2, [0015], where analysis platform collects configuration files from the relevant network devices and builds up an internal instance of a network configuration model based on the configuration files and the network topology which relates to network DNA policy condition referencing network DNA component); and

an execution of a network DNA policy action of the network DNA policy if the network DNA policy condition of the network DNA policy is satisfied (Meyer, Fig.2, where the analysis platform receives the network policy as an input and then analyzes the network configuration model to verify that the IP traffic from and to these hosts are limited according to the type of service, and to ensure that the right type of IP traffic get from/to a host, which includes the configuration of relevant routers for switching traffic, firewalls for passing through or dropping traffic, and local access control mechanisms on the host (e.g., TCP wrappers) for making the services accessible).

11. Claims 20, 40-41 carry similar limitations as claim 16 and 22 above and therefore are rejected under for same rationale.

12. Claim 2 is rejected under 35 U.S.C 103 (a) as being unpatentable over Tezuka, Meyer and Delo in views of Jemes.

13. As to claim 2, Tezuka, Meyer and Delo discloses the invention substantially as in parent claim 1 above, including, wherein said at least one derived network DNA component comprises a network species component (Tezuka, Fig.2, [0035], It is obvious that any network contains species component). Tezuka, Meyer and Delo however are silent on disclosing explicitly, indicating a network species classification , the network species classification comprising one of an enterprise network , home network and a public network.

Jemes however discloses a similar concept where, indicating a network species classification , the network species classification comprising one of an enterprise

network , home network and a public network (Jemes, [0017], where network policy defines the security level of the network to which it is connected, e.g. different security level of different network as depicted in Fig.2).

Therefore it would have been obvious to one of the ordinary skilled in the art at the time the invention was made to combine the teachings of Tezuka, Meyer and Delo with the teachings of Jemes in order to provide a system which includes a plurality of networks where each network has at least one network device configured to transmit and receive data and has a network security policy. The secure network further includes a plurality of network control points where each network control point has at least one network control point device. Each of the plurality of network control points is connected to at least one of the plurality of networks.

14. Claims 3-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tezuka, Meyer and Delo as applied to claim 1 above in view of Anderson.

15. As to claim 3, Tezuka, Meyer and Delo discloses the invention substantially as applied to claim 1 above, including, wherein at least one of said at least one derived network DNA component specification comprises at least one value of at least one of said at least one raw network DNA component.

Tezuka, Meyer and Delo however is silent on, “a linear transformation”.

Anderson however discloses, "a linear transformation" (Anderson, [0186], where network confidence level is Network DNA component is calculated based on linear combination of each of constituent confidence factor field).

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Tezuka, Meyer and Delo with the teachings of Anderson in order to provide a hierarchy of network DNA with respect to network DNA confidence level which will help developing network architectural models in future.

16. As to claim 4, Tezuka, Meyer, Delo and Anderson discloses the invention substantially, including, wherein said at least one derived network DNA component specification comprises a combination of said at least one raw network DNA component (Anderson, [0186], where confidence factors are combination of raw and derived network DNA).

17. Claims 5-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tezuka, Meyer and Delo in view of Beadles et al. (Patent No.: US 7159125 B2), hereinafter “Beadles”.

18. As to claims 5-7, Tezuka, Meyer and Delo disclose the invention substantially as in parent claim 1 above. Tezuka, Meyer and Delo however is silent on disclosing, “wherein at least one of said at least one derived network DNA component specification comprises a structured query language statement”.

Beadles however, discloses, "wherein at least one of said at least one derived network DNA component specification comprises a structured query language statement" (Beadles, Col.7, lines 5-6, where Network policy store/Network DNA is implemented as SQL server database, further these policy's can be written in any other well known languages in the art e.g. pearl, Visual basic etc.).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Tezuka, Meyer and Delo with the teachings of Beadles in order to provide device management policy to have control over network via developing a policy to associated network devices.

19. As to claims 8-9, Tezuka, Meyer, Delo and Beadles disclose the invention substantially as in claim 5-7 above, including, wherein acquiring at least one raw network DNA component comprises acquiring a plurality of raw network DNA components in an order specified by a raw network DNA acquisition priority list (Beadles, NAT Directory schema, Col.23 and 24, Abstract, where multiple hierarchical services which are plurality of network DNA components and from hierarchy may priorities can be extracted e.g. reliability, security, confidence level etc. further it will be obvious make the hierarchy policy based).

20. Claims 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tezuka, Meyer and Jemes as applied to claim 16 above in view of Jacobs et al. (Patent No.: US 7257560 B2), hereinafter "Jacobs".

21. As to claims 18-19, Tezuka, Meyer and Jemes discloses the invention substantially as in parent claim 16, including, wherein the network DNA further comprises a network name component (Tezuka, [0006], where network comprises of single technology domain, e.g. IP, SDH or access etc and IP address is operational attribute as well), a core access component (Tezuka, Fig.3, N1 and N2 are access network), a core addressing component (Tezuka, [0041], where IP network is addressing component), a network security component (Meyer, [0005], where firewall is a security component) and a network technology component (Tezuka, [0041], where IP, SDH are network technology component).

Tezuka, Meyer and Jemes however are silent on disclosing explicitly, "a network cost component".

Jacobs however discloses, "a network cost component" (Jacobs, [0014], where associated cost to network utilization is disclosed.

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Tezuka, Meyer and Jemes as applied to claim 16 above, with the teachings of Jacobs in order to provide a technique to track the costs associated with different service providers for service utilizations.

22. Claims 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tezuka, Meyer and Delo as applied to parent claim1 in view of Marples et al. (Pub. No.: US 2003/0140142 A1), hereinafter "Marples".

23. As to claims 13-15, Tezuka, Meyer and Delo disclose the invention substantially as in claim 1. Tezuka, Meyer and Delo however are silent on disclosing explicitly, “wherein the network DNA policy reduces performance penalties when switching between computer networks”.

Marples, however discloses, “wherein the network DNA policy reduces performance penalties when switching between computer networks” (Marples, [0004], where firewall is placed between private and public network and enforcing access control policy for security concerns).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Tezuka, Meyer and Delo as applied to parent claim 1 above with the teachings of Marples "Access control policy for security concerns” in order to provide a switching capability between private and public network on the fly without having to worry about security concerns.

24. Claims 12, 17, 23 and 25-26 and 28-37 are rejected under 35 U.S.C 103 (a) as being unpatentable over Tezuka, Meyer and Jemes in views of Williams et al. (Pub. No.: US 2005/0257267 A1), hereinafter "Williams".

25. As to claims 12 and 31, Tezuka, Meyer and Jemes disclose the invention substantially as in claim 1 and 27 above, including, testing network policy condition (Meyer, [0015], The analysis platform collects configuration files from the relevant network devices and builds up an internal instance of a network configuration model based on the configuration files and the network topology).

Tezuka, Meyer and Jemes however are silent on disclosing explicitly, whether sufficient network DNA referenced by the DNA network policy condition of the network DNA policy has been acquired.

Williams however discloses, whether sufficient network DNA referenced by the DNA network policy condition of the network DNA policy has been acquired (Williams, [0099], where testing one of the selected policy from test menu implies testing different policy to see if acquired data is sufficient).

Therefore, it would have been obvious to one of ordinary skilled in the art at the time the invention was made to combine the teachings of Tezuka, Meyer and Jemes with the teachings of Williams in order to provide a network auditing system for auditing the security of a data communications network.

26. As to claim 17, Tezuka, Meyer, Jemes and Williams disclose the invention substantially, including, generating at least one derived network DNA component according to at least one derived network DNA component specification (Tezuka, Fig.3, [0043], where SDH network N3 accommodates network element designed for SDH transmission thus formulating a single technology domain, which is N3 domain will be used for N3 like domain preferences) at least one of said at least one derived network DNA component specification referencing at least one acquirable attribute of the computer network (Tezuka, [0043], it is obvious that, “SDH network N3 accommodates network element designed for SDH transmission thus formulating a single technology domain” these derived network preferences have been build on existing network retrieved preferences or network DNA component).

27. As to claim 23, Tezuka, Meyer, Jemes and Williams disclose the invention substantially as in parent claim 22, including, wherein said at least one network DNA store comprises a current network DNA store and a network DNA history store (Tezuka, [0039], where updated network management model is saved into database).

28. As to claim 25, carry similar limitations as parent claim 22, therefore is rejected under for same rationale.

29. As to claim 26, Tezuka, Meyer, Jemes and Williams disclose the invention substantially as in parent claim 22, including, wherein each network DNA policy comprises a derived network DNA components dependency list that lists each derived network DNA component of the network DNA referenced by the network DNA policy (Williams, [0072, lines 1-6], where policy library-42 is a repository of pre-established policies, therefore it is obvious that any network build on these policies will be derived and dependent on these policies).

30. As to claim 28, Tezuka, Meyer, Jemes and Williams disclose the invention substantially as in parent claim 27, including, wherein the network DNA policy condition of the network DNA policy is satisfied if an expression specified by the network DNA policy condition evaluates to Boolean true (Williams, Fig.12A, policy violation-916, [0135], where complying with the policy is “Boolean true”, which handle the violation per policy instruction).

31. As to claim 29, Tezuka, Meyer, Jemes and Williams disclose the invention substantially as in parent claim 27, including, wherein the network DNA policy condition of the network DNA policy is satisfied if an expression specified by the network DNA policy condition evaluates to Boolean false (Williams, Fig.12A, policy violation-916, [0135], where not complying with the policy in false, which terminates the process).

32. As to claim 30, Tezuka, Meyer, Jemes and Williams disclose the invention substantially as in parent claim 27, including, wherein the network DNA policy condition of the network DNA policy is satisfied if evaluating an expression specified by the network DNA policy condition results in an evaluation error (Williams, [0068], where policy evaluation is tested before deployment, which obviously is an essential step of removing any remaining errors in policy).

33. As to claims 32, Tezuka, Meyer, Jemes and Williams disclose the invention substantially as in parent claim 27, including, each network DNA component is associated with a confidence level (Williams, Fig.3, recommendation engine, [0078], where recommendation engine is provide a confidence level and each policy is associated with confidence level); and

sufficient network DNA has been acquired for the network DNA policy if the confidence level of each network DNA component referenced by the network DNA policy condition of the network DNA policy is greater than zero (Williams, [0144], where mapping score is above a given threshold and where threshold can be a zero).

34. As to claim 33-34, carry similar limitation as claim 32 above and therefore, are rejected under for same rationale.

35. As to claim 35, Tezuka, Meyer, Jemes and Williams disclose the invention substantially as in parent claim 22, including, a network DNA generator configured to, at least generate said at least one derived network DNA component according to at least one derived network DNA component specification (Tezuka, Fig.3, [0043], where SDH network N3 accommodates network element designed for SDH transmission thus formulating a single technology domain, which is N3 domain will be used for N3 like domain preferences) at least one of said at least one derived network DNA component specification referencing at least one raw network DNA component of the network DNA associated with the computer network (Tezuka, [0043], it is obvious that, "SDH network N3 accommodates network element designed for SDH transmission thus formulating a single technology domain" these derived network preferences have been build on existing network retrieved preferences or network DNA component).

36. As to claim 36, Tezuka, Meyer, Jemes and Williams disclose the invention substantially as in parent claim 35, including, wherein the network DNA generator is further, at least, configured to maintain at least one derived-raw network DNA component dependency list (Tezuka, [0038], where existing network scenarios are stored in database), said at least one derived-raw network DNA component dependency list comprising (Tezuka, [0038], where scenarios are dependency list), for each derived network DNA component generated by the network DNA generator

(Tezuka, [0038], where model builder is DNA generator which generates or updates new models), a list referencing each raw network DNA component referenced by each derived network DNA component specification associated with the derived network DNA component (Tezuka, [0038], obviously these derived network models are based on existing network scenarios and therefore new models history and log will be referencing back to the existing network or base network model or architectures).

37. As to claim 37, Tezuka, Meyer, Jemes and Williams disclose the invention substantially as in parent claim 35, including, wherein the network DNA generator is further (Tezuka, [0010], where network management model builder is network DNA generator), at least, configured to generate each derived network DNA component referenced by a derived network DNA refresh list (Tezuka, [0010], where network builder further updates/refresh the model in response to a network construction request), the derived network DNA refresh list referencing each derived network DNA component dependent upon a changed raw network DNA component (Tezuka, [0010], where any changes to these component are stored in a database which is equivalent too log or history of data over a period of time).

38. Claims 38-39 are rejected under 35 U.S.C 103(a) as being unpatentable over Tezuka, Meyer and Jemes as applied to claim 22 above in view of Britt et al. (Patent No.: 6,675,209 B1), hereinafter “Britt”.

39. As to claim 38, Tezuka, Meyer and Jemes discloses the invention substantially as in parent claim 22 above, including, “acquiring a plurality of raw network DNA

component" (Tezuka, [0036], where request is send out to collect network preferences). Tezuka, Meyer and Jemes however are silent on disclosing explicitly, "acquirer, acquire network DNA component according to priority list specified by raw network DNA acquisition priority list" or "each raw network DNA component corresponding to an attribute of said at least one computer network".

Britt however discloses, "acquirer, acquire network DNA component according to priority list specified by raw network DNA acquisition priority list" (Britt, Claim 16) or "each raw network DNA component corresponding to an attribute of said at least one computer network" (Britt, Claim 16).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Tezuka, Meyer and Jemes with the teachings of Britt in order to provide an adaptive system module includes a network organizer that categorizes the multiple segments of the network, a network prioritizer that ranks the categorized segments amongst themselves according to a necessity to obtain data traffic information for analysis, and a system optimizer that determines how many of the ranked segments can provide data traffic information within a set protocol data unit ("PDU") credit limit.

40. As to claim 39, Tezuka, Meyer, Jemes and Britt discloses the invention substantially as in parent claim 38, including, wherein the order specified by the raw network DNA acquisition priority list is in accord with an ordered set of network DNA policies that reference the plurality of raw network DNA components (Tezuka, Fig.6,

Tributary-11a, [0054], where network DNA is listed sequentially which is the result of applied policies of raw network DNA).

41. Claim 42 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tezuka, Meyer and Jemes as applied to claims 40 and 41 above in view of Jacobs et al. (Patent No.: US 7257560 B2), hereinafter "Jacobs".

42. As to claim 42, Tezuka, Meyer and Jemes discloses the invention substantially as in parent claim 40, including, wherein the network DNA further comprises a network name component (Tezuka, [0006], where network comprises of single technology domain, e.g. IP, SDH or access etc and IP address is operational attribute as well), a core access component (Tezuka, Fig.3, N1 and N2 are access network), a core addressing component (Tezuka, [0041], where IP network is addressing component), a network security component (Marples, [0005], where firewall is a security component) and a network technology component (Tezuka, [0041], where IP, SDH are network technology component).

Tezuka, Meyer and Jemes however are silent on disclosing explicitly, "a network cost component".

Jacobs however discloses, "a network cost component" (Jacobs, [0014], where associated cost to network utilization is disclosed.

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Tezuka, Meyer and Jemes as

applied to claim 40 above, with the teachings of Jacobs in order to provide a technique to track the costs associated with different service providers for service utilizations.

43. Claims 43-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tezuka, Meyer, Jemes and Jacobs as applied to claims 40 and 41 above in view of Anderson et al. (Pub. No.: US 2004/0068582 A1), hereinafter "Anderson".

44. As to claim 43, Tezuka, Meyer, Jemes and Jacobs disclose the invention substantially as in parent claim 40. Tezuka, Meyer, Jemes and Jacobs however are silent on disclosing explicitly, "wherein the network DNA further comprises a confidence level for each of the at least one network classification component".

Anderson however, discloses, "wherein the network DNA further comprises a confidence level for each network classification component" (Anderson, Fig.28, [00196], where fuzzy and crisp logic with confidence level is disclosed).

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to combine the teachings of Tezuka, Meyer, Jemes and Jacobs with the teachings of Anderson in order to provide a hierarchy of network DNA with respect to network DNA confidence level which will help developing network architectural models in future.

45. As to claim 44, Tezuka, Meyer, Jemes, Jacobs and Anderson discloses the invention substantially as in parent claim 40 above, including, at least one value of at least one of the network classification component is determined probabilistically (Anderson, [0196], where network address is located probabilistically); and the

confidence level of said at least one of at least network classification component determined probabilistically corresponds to a margin of error in the determination (Anderson, Fig.28, [0196], where probability means result is based on margin of error).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TAUQIR HUSSAIN whose telephone number is (571)270-1247. The examiner can normally be reached on 7:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571 272 3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/T. H./
Examiner, Art Unit 2452

/Kenny S Lin/
Primary Examiner, Art Unit 2452